**Fınal Exam CMSE-512 20.06.2025, 16.30 (150 min, 100 points)**

St. Name, Surname\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ St.Id#\_\_\_\_\_\_\_\_\_\_\_\_\_

**Five A4-sized cheat sheets with your handwritten notes may be used. Calculators are allowed. Telephones and other electronic devices are not allowed**

Instructor Alexander Chefranov

**Totally 11 questions, 13 pages**

Good Luck!

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Name Surname | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | Total |
| Point | 3 | 4 | 12 | 7 | 7 | 8 | 8 | 20 | 12 | 12 | 7 | 100 |
| Grade |  |  |  |  |  |  |  |  |  |  |  |  |

**Before MT Exam tasks 1-5 (33 points)**

**Task 1 (3 points)** Explaın why anonymity is an ımportant security requırement

Anonymity is important because if information, activity, transactions is attributed to a particular person it can be used for harm

**Task 2. (4 points)** What four password breaking methods do you know? Explain each of them briefly

1. Try short sequences of 1-2-3 symbols from the keyboard
2. Try user’s name, names of his/her spouse, children, their birthdays, pets’ names, car plates, etc.
3. Try dictionary words
4. Try slight changes of the dictionary words (capitalize letters, change O by 0, I by 1, add digits)

**Task 3. (12 points)** Define an RSA private/public key pair if N=119, and encrypt the plaintext M=3. Use successive squaring and immediate modulo reduction for encryption. Show details of your calculations, give necessary explanations.

**Hints**: Two large prime numbers, *p* and *q*, , are selected, and an integer, *d*, is chosen that is relatively prime to *(p-1)(q-1)*. Finally, an integer e is computed such that

, N=pq, C=MemodN, M=CdmodN

EXTENDED EUCLID(m,b)

1. (A1,A2,A3):=(1,0,m); (B1,B2,B3):=(0,1,b);
2. if B3=0 return A3=gcd(m,b); no inverse
3. if B3=1 return B3 = gcd(m,b); B2= b-1 mod m
4. Q=
5. (T1,T2,T3):=(A1-QB1, A2-QB2, A3-QB3)
6. (A1,A2,A3):= (B1,B2,B3)
7. (B1,B2,B3):= (T1,T2,T3)
8. goto 2

**Immediate modulo reduction**: a\*b mod m = ((a mod m) \* (b mod m)) mod m

**Successive squaring**: a^8 = ((a^2)^2)^2

N=119 = p\*q= 7\*17=>p=7, q=17; fi(N)=(p-1)(q-1)=6\*16 = 96

Let e= 5, then d= e^(-1) mod 96 = 5^(-1) mod 96, d=77. Check it: 5\*77 = 385 = 96\*4+1 mod 96 =1

Find it by EEA:

A=(1,0,96), B=(0,1,5)

Q=floor(96/5) = 19

T=A-qB = (1-19\*0, 0-19\*1, 96-19\*5) = (1,-19, 1)

A=B=(0,1,5)

B=T=(1,-19,1)

B3=1=>B2=-19 mod 96 = 77 = d

C=M^e mod 119 = 3^5 mod 119 = 243 mod 119 = 2\*119 +5 mod 119 = 5

**Task 4. (7 points)** Which bits of the 2nd round right half input R1 are defined by the outputs 2 and 3 of the S-box S4 of the first round of DES? Fill in the Answer table below. Explain your answer

**Hints**:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |

|  |
| --- |
| Permutation function( P ) |
| 16 7 20 21 29 12 28 171 15 23 26 5 18 31 102 8 24 14 32 27 3 919 13 30 6 22 11 4 25 |

 |

Answer table:

|  |  |  |
| --- | --- | --- |
| S-box number | S-box output number | Bit # of R1 |
| 4 | ~~1~~ 2 | 20 |
| 4 | ~~2~~ 3 | 10 |

S4 outputs 2, 3 after combining comprise outputs 14, 15 respectively from the S-boxes.

According to P, S-boxes output 14 goes to the position 20, and 15 goes to the position 10. Hence, outputs 2, 3 of S4 affect bits 20 and 10 of R1.

**Task 5. (7 points)** Explain how the 64-bit registers *a,b,c,d,e,f,g,h* are initialized in SHA-512. Calculate the first three hexadecimal digits, A54, of the register d. Show your calculations, explanation them

**Hints**:





The registers are initialized by the first 64 bits of the fractional parts of the square roots of the first 8 prime numbers which are 2,3,5,7,11,13,17, and 19. Register d is initialized using 7

$\sqrt{7}=$2,6457513110645905905016157536393. Multiply its fractional part by 16

0,6457513110645905905016157536393\*16 = 10,332020977033449448025852058228. Its integer part 10 =A, the 1st hexadecimal digit of d. Again, multiply the fractional part of the result by 16:

0,332020977033449448025852058228\*16 =5,3123356325351911684136329316507. Its fractional part is 5, the 2nd hexadecimal digit of d. Again, multiply the fractional part of the result by 16:

0,3123356325351911684136329316507\*16 = 4,9973701205630586946181269064107. It fractional part is 4, i.e. the 3rd hexadecimal digit of d.

**After MT Exam tasks 6-11 (67 points)**

**Task 6. (8 points)**  Explain what for and how the in the message M3 of the Kerberos protocol is used?

**Hints:**



The authenticator is used to check that the client requesting a service is valid. It is checked decryption with the session key shared by the client and server: 1) client’s name, C, shall be the same as in the ticket; 2) timestamp, TS, shall be not expired; 3) TS shall be used for the first time.

**Task 7. (8 points)** How many actors are in the SET protocol? What are their responsibilities? Which actors of the SET protocol have certificates and what for?

**Hints:**

“Before SET begins, C and M negotiate the terms of a purchase. The protocol begins with a handshake in which C and M exchange certificates and authenticate each other. C sends its certificate to M, and M sends both its certificate and G’s certificate to C, at which point C and M know each other’s and G’s public key. Then the purchase transaction begins.

1. M sends a signed message to C containing a (unique) transaction Id (which is used to guard against replay attacks). C uses the public key in M’s certificate to check the signature and hence knows that the message came from M and was not altered in transit.
2. C sends a message to M containing two parts plus the dual signature:
3. The transaction Id, C’s credit card information, and the dollar amount of the order (but not a description of the items purchased) – encrypted with G’s public key:



1. The transaction Id, the dollar amount of the order, a description of the items purchased (but not C’s credit card information) – encrypted with M’s public key:



The dual signature has three fields:

1. The message digest, MD1, of the first part of the message:



where f is the message digest function

1. The message digest, MD2, of the second part of the message:



1. C’s signature of the concatenation of MD1 and MD2:



Thus, the complete dual signature is



and the complete message sent from C to M is .

The dual signature binds the two parts of the message. So, for example, an attempt by an intruder or M to associate  with  does not work since its message digest, MD2’, will differ from MD2. Although MD2’ can be substituted for MD2 in the dual signature,  cannot be used as the signature for MD1\*MD2’, and only C can compute the correct dual signature for the reconstructed message.

1. M decrypts the second part of the message with its private key (but it cannot decrypt the first part, which contains the credit card number). The merchant then
2. Uses the dual signature to verify that has not been altered in transit. It first computes the message digest of  and checks that it is the same as the second field of the digital signature (MD2). It then uses the public key in C’s certificate to check that the third field is the correct signature for the concatenation of the first two fields.
3. Verifies the transaction Id, the dollar amount of the order, and the description of the items purchased

Next M sends a message to G containing two parts:

(a)  and the dual signature it received from C:



1. The transaction Id and the dollar amount of the order – signed with M’s private and encrypted with G’s public key:



The complete message sent from M to G is , together with copies of C’s and M’s certificates

1. G decrypts the message using its private key.
2. It uses the dual\_signature and the public key in C’s certificate to verify that  was prepared by C and was not altered (as in step 3a).
3. It uses the message digest of the credit card information in C’s certificate to verify the credit card number supplied in .
4. It uses M’s signature in and the public key in M’s certificate to verify that  was not altered
5. It checks that the transaction Id and the dollar amount are the same in  and  (to verify that M and C agreed on the purchase)
6. It checks that the transaction Id was never submitted before (to prevent a replay attack)
7. It does whatever is necessary to approve the credit card request

Then G returns a signed approved message to M. At this point, the transaction is committed.

1. When M receives the approved message, it knows that the transaction has committed. It sends a signed message to C: transaction complete. C then knows that transaction has committed.”

The actors of SET protocol are: Client, Merchant, and Payment Gateway. The Payment Gateway is responsible for checking that Merchant and Customer both agree on the transaction with same particular ID number and amount of money, checks that the transaction ID is not repeated, checks validity of the Client credit card, debits Client’s credit card, and credits Merchant’s account. The dual signature is Client’s digital signature of the message digests of the messages m1 and m2 sent by Client to Merchant. The dual signature is used by Payment Gateway to check that m1 was prepared by Client and was not altered.”

There are three actors in the SET protocol: Client, Merchant, and Payment Gateway. The Payment Gateway is responsible for checking that Merchant and Customer both agree on the transaction with same particular ID number and amount of money, checks that the transaction ID is not repeated, checks validity of the Client credit card, debits Client’s credit card, and credits Merchant’s account. Client is responsible for sending Merchant a two-part message bound by created by him/her dual signature. Merchant is responsible for providing Client with unique transaction ID, checking m2, and sending m1 and his/her confirmation of the transaction to Payment gateway. All the actors have certificates and use them to have trusted other parties’ public keys used for encryption and for digital signature validation. Cient’s certificate also has the credit card information verified by Payment Gateway

**Task 8. (20 points)** Given RSA public/private keys (5,91)/(29,91) and a valid serial number, $sn=23$, blind it, make a blinded token, and, un-blinding it,get a valid token, and check it validness assuming that the validity predicate is $valid(sn)= (sn mod 10 ==3)$.

**Hints**:

# “Creating a Blinding Function

The protocol requires that C creates his own blinding function, *b*, unknown to B. This might seem a difficult task, but it is actually quite easy in the context of RSA algorithm for public key cryptography. In one scheme for doing this, C first generates a random number, *u*, that is relatively prime to the modulus *N* of the bank’s keys. Because u is relatively prime to *N*, it has a multiplicative inverse, , with respect to *N*, such that



To blind the serial number, *n*, C computes



and sends the result to B. Hence, the blinding function can be viewed simply as multiplication by a random number.

The signed result, *sr*, returned by B to C is



Obviously, . To recover the token, we use



The serial number *n* can be now obtained using.”

Select u=2, u^(-1) mod 91 = 46. Blinded serial number bsn= 2^5\*23 mod 91 = 32\*23 mod 91 = 8\*4\*23 mod 91 = 8\*92 mod 91 = 8

Blinded token btn = bsn^29 mod 91= 8^29 mod 91

29=16+8+4+1

8^2 = 64 mod 91 =64

8^4 = 64\*64 mod 91 = 32\*128 mod 91 = 32\*37 mod 91 = 16\*74 mod 91 = -16\*17 mod 91 = -2\*136 mod 91 = - 2\*45 mod 91 = -90 mod 91 = 1

8^8 =1

8^16 =1

Hence, btn = 8^29 = 8^16\*8^8\*8^4\*8 mod 91 = 1\*1\*1\*8 mod 91 = 8.

Unblinded token, utn = u^(-1)\*btn mod 91 = 46\*8 mod 91 = 92\*4 mod 91 = 4

Decrypting utn by the public key 5, we get back original serial number sn’=utn^5 mod 91 = 4^5 mod 91 = 128\*8 mod 91 = 37\*8 mod 91 = 74\*4 mod 91 = -17\*4 mod 91 = -68 mod 91 = 23 = sn

Valid (sn) = sn mod 10 = 3, hence, it is valid.

**Task 9. (12 points)** Assuming that the hash function $h\left(x\right)=\left⌈\frac{x^{2}}{3}\right⌉ mod 31+17$, where $\left⌈x\right⌉$ is ceiling of $x$, i.e, the minimal integer not less than $x$, $p\_{0}=5$, and $N=4$, calculate $p\_{N}$ for the Lamport’s One-time password scheme. Show details of your calculations and explain them.

**Hints**:

# Initialization Procedure

The client selects a password, , a number, , calculates

,

where

.

p1=h(p0) = $\left⌈\frac{p0^{2}}{3}\right⌉ mod 31+17$=$\left⌈\frac{25}{3}\right⌉ mod 31+17$ = 9+17 = 26

p2=h2(p0) = $\left⌈\frac{26^{2}}{3}\right⌉ mod 31+17$=$\left⌈225.3\right⌉ mod 31+17$=$226 mod 31+17$ = 9+17 = 26

p3= h3(p0) = $\left⌈\frac{26^{2}}{3}\right⌉ mod 31+17$=$226 mod 31+17$ = 9+17 = 26

p4= h4(p0) = $\left⌈\frac{26^{2}}{3}\right⌉ mod 31+17$=$226 mod 31+17$ = 9+17 = 26

Hence. p4=26

**Task 10. (12 points)** Explain SQL Injection attack using an example from the Lecture notes below:

“A bank might have an application that allows a user to download all transactions involving the user’s account. After the application identifies and authenticates the user, it might compose a query for the user on the order of

QUERY = “SELECT \* FROM trans WHERE acct=’”+ acctNum + ”’;”

Because the communication is between an application running on a browser and the web server, the query is encoded within a long URL string

[http://www.mybank.com?QUERY=SELECT%20\*%20FROM%20trans%20WHERE%20acct=‘2468](http://www.mybank.com?QUERY=SELECT%20*%20FROM%20trans%20WHERE%20acct='2468)’

In this command, the space character has been replaced by its numeric equivalent %20 (because URLs cannot contain spaces), and the browser has substituted ‘2468’ for the account number variable. The DBMS will parse the string and return records appropriately. If the user can inject a string into this interchange, the user can force the DBMS to return a set of records. The DBMS evaluates the WHERE clause as a logical expression. If the user enters the account number as

“‘2468’ OR ‘1’=‘1’”

the resulting query becomes

QUERY = “SELECT \* FROM trans WHERE acct=’”+ acctNum + ”’;”

and after account number expansion it becomes

QUERY = “SELECT \* FROM trans WHERE acct=‘2468’OR ‘1’=‘1’”

“

 SQL injection attack tries entering such data that the conditional used in WHERE clause evaluates to 1 (True). In the above example it is made by extending the condition acct=‘2468’by OR ‘1’=’1’ that yields an expression acct=‘2468’OR ‘1’=’1’ true for any record, hence, all the records are selected to the result set.

**Task 11. (7 points)** Statistical databases (SDB) can be protected using perturbation as illustrated in the figure below



Explain how Perturbated SDB could be obtained from the original SDB.

SDB has sensitive and insensitive attributes. Sensitive attributes shall be hidden by perturbation. It can be made by evaluating a probability distribution of the sensitive attributes, and randomly generating their values according to the probability distribution obtained.